CLAIMS

What is claimed is:

1. An apparatus for performing network routing, the apparatus comprising:

authentication logic configured to receive packets sent from a source agent to an endpoint of a tunnel and to determine whether a security association of a packet received corresponds to said source agent, the tunnel being configured by said source agent in accordance with a network protocol;

decision logic configured to make a routing decision for each authenticated packet that is constrained based on the security association of the authenticated packet; and

routing logic configured to select a routing destination for each authenticated packet and to route the authenticated packet to the selected routing destination, the routing destination selection being based at least partially on said routing decision.

2. The apparatus of claim 1, wherein the routing destination selection is based solely on said routing decision.

3. The apparatus of claim 1, further comprising:

decapsulation logic configured to decapsulate received packets, wherein when the decapsulation logic decapsulates a packet, the security association of the packet is preserved and contents of a payload of an authenticated packet are routed to the selected routing destination.

4. The apparatus of claim 1, wherein the network protocol is Internet Protocol Security (IPSec) Protocol (IPSEP).

5. The apparatus of claim 1, wherein the network protocol is a public network protocol.

6. The apparatus of claim 1, wherein the network protocol is a private network protocol.

7. The apparatus of claim 1, wherein said routing decision is a decision to route at least a portion of contents of a payload of an authenticated packet to a layer 3 device, wherein layer 3 corresponds to a particular layer of Open Systems Interconnect (OSI) networking model.

8. The apparatus of claim 7, wherein the layer 3 device is a router.

9. The apparatus of claim 1, wherein said routing decision is a decision to route at least a portion of contents of a payload of an authenticated packet to a layer 2 device, wherein layer 2 corresponds to a particular layer of Open Systems Interconnect (OSI) networking model.

10. The apparatus of claim 9, wherein the layer 2 device is a switch.

11. The apparatus of claim 10, wherein the switch is comprised by a Virtual Local Area Network (VLAN).

12. The apparatus of claim 1, wherein the decision made by the decision logic is a decision whether to route at least a portion of payload contents of an authenticated packet to a layer 2 device or to a layer 3 device, wherein layers 2 and 3 correspond to particular layers of Open Systems Interconnect (OSI) networking model.

13. The apparatus of claim 1, wherein said routing decision is made by said decision logic without regard to the contents of the authenticated packet.

14. The apparatus of claim 1, wherein an authentication ID is derived from said security association, and wherein said routing decision is constrained based on said authentication ID.

15. A method for performing network routing, the method comprising the steps of:

authenticating received packets sent from a source agent to an endpoint of a tunnel by determining whether a security association of a received packet corresponds to the source agent that sent the packet, the tunnel being configured by said source agent in accordance with a network protocol;

making a routing decision for an authenticated packet, the routing decision being constrained based on the security association of the authenticated packet;

selecting a routing destination for a packet based at least partially on the routing decision; and

routing the authenticated packet to the selected routing destination.

16. The method of claim 15, further comprising the step of:

decapsulating the packets, wherein when the packet is decapsulated, contents of a payload of the authenticated packet are decapsulated and the security association of the packet is preserved.

17. The method of claim 15, wherein the network protocol is Internet Protocol Security (IPSec) Protocol (IPSEP).

18. The method of claim 15, wherein said routing decision is a decision to route at least a portion of payload contents of the authenticated packet to a layer 3 device, layer 3 corresponding to a particular layer of an Open Systems Interconnect (OSI) networking model.

19. The method of claim 18, wherein the layer 3 device is a router.

20. The method of claim 15, wherein said routing decision is a decision to route at least a portion of payload contents of an authenticated packet to a layer 2 device, layer 2 corresponding to a particular layer of an Open Systems Interconnect (OSI) networking model.

21. The method of claim 20, wherein the layer 2 device is a switch.

22. The method of claim 21, wherein the switch is comprised by a Virtual Local Area Network (VLAN).

23. The method of claim 15, wherein the routing decision is a decision as to whether to route at least a portion of payload contents of an authenticated packet to a layer 2 device or to a layer 3 device, wherein layers 2 and 3 correspond to particular layers of an Open Systems Interconnect (OSI) networking model.

24. A computer program for performing network routing in accordance with a private network security technique, the computer program being embodied on a computer readable medium, the computer program comprising:

a first code segment, the first code segment authenticating received packets sent from a source agent to a tunnel endpoint to determine whether a security association of a received packet corresponds to the source agent that sent the packet, the tunnel being configured by said source in accordance with a network protocol;

a second code segment, the second code segment making a routing decision for an authenticated packet, the routing decision being constrained based on the security association of the authenticated; and

a third code segment, the third code segment selecting a routing destination for the authenticated packet based at least partially on the routing decision made by the second code segment.

25. The computer program of claim 24, further comprising:

a fourth code segment that is executed before the second code segment, the fourth code segment performing a decryption algorithm that attempts to decrypt the authenticated packet prior to the second code segment making a routing decision, wherein when the decryption algorithm is successful at decrypting the authenticated packet, contents of a payload of the authenticated packet are decrypted and the security association of the decrypted packet is preserved for use by the second code segment in making the routing decision.